Committee on Ways and Means, Subcommittee on Social Security
Hearing on Identity Theft – April 13, 2011
Questions for the Record

1) The President's Identity Theft Task Force recommended that the Social Security Administration (SSA) become a clearinghouse for federal agencies that minimize the use of SSNs by the fourth quarter of 2007. What progress can you report on this recommendation?

The Task Force's recommendation read:

> **"Establish a Clearinghouse for Agency Practices That Minimize Use of SSNs"**
> To encourage agencies to share best practices on minimizing the use of SSNs, the Task Force recommended that we develop a clearinghouse to promote successful government initiatives in this area and to facilitate information sharing. The Task Force made the recommendation to build upon OMB's recent review of how agencies use SSNs, as well as to leverage successful efforts across the Federal government.

We implemented this recommendation in two steps. First, we formed the Social Security Number (SSN) Best Practices Collaborative, which included representatives from 36 Federal departments and agencies and met regularly in 2007 to explore, develop, and share best practices for reducing reliance on SSNs. The Collaborative formed a subcommittee chaired by the Internal Revenue Service (IRS) and comprised of agencies that handle high volumes of SSNs and personally identifiable information (PII), such as the Department of Defense, Department of Veterans Affairs, the Department of Homeland Security (DHS), the Centers for Medicare and Medicaid Services (CMS), and us.

Second, we established a clearinghouse on a bulletin board website in July 2007; over 25 agencies have registered as users to date. The clearinghouse, which remains operational and is located at www.idtheft.gov/takeaction.html, provides a forum to share materials regarding SSN use and display by Federal agencies. It highlights best practices as well as contacts for specific programs and initiatives.

2) What is SSA doing to end the practice of K-12 schools collecting students' SSNs and using them as authenticators?

We actively encourage schools and universities, as well as other entities, to reduce the unnecessary collection of SSNs by:

- Establishing a website with links to our publications, policy, frequently asked questions (FAQs), and best practices for protecting SSNs and promoting our website to State and local governments as part of our on-going educational outreach efforts;
- Coordinating with State Departments of Education and K-12 school systems to inform the education community about the potential risks of using the SSN as a student identifier;

- Encouraging State Departments of Education and K-12 school systems to implement safeguards to protect SSNs when collected; and
- Promoting the best practices States and K-12 school systems have taken to limit the use of the SSN.

We also publish pamphlets, such as *Your Social Security Number and Card,* that tell individuals not to carry their SSN card. The pamphlet also advises individuals to avoid giving out their SSN unnecessarily.

- These publications are available in our field offices and on our website.
- They also are available free of charge through the Federal Citizen Information Center in Pueblo, Colorado.

In addition, we post FAQs on our website that address identity theft and how we protect SSNs. About 50,000 people view these FAQs each month.

3) How does the SSA alert or educate cardholders on the proper protection of their SSNs? Do you inform the public on how to protect their SSNs? Does SSA conduct public outreach to institutions and businesses with respect to the display of SSNs? Does the agency provide best practices information for the handling of personal data?

We take the protection of SSNs very seriously. We keep our records confidential and disclose information only when the law permits.

We routinely inform and remind the public about ways they can protect their SSNs:

- We advise individuals to be careful about sharing their SSNs with others, even when requested;
- We encourage individuals to keep their SSN card in a safe place and not carry the card, or any document displaying their SSN, with them;
- We offer pamphlets that tell individuals not to carry the SSN card unless an employer or service provider insists on seeing it, and to avoid giving out their SSN unnecessarily (see response to question 2 for links to specific publications and the Federal Citizen Information Center);
- We post FAQs on our website that address identity theft and how we protect SSNs. About 50,000 people view these FAQs each month;
- We write stories for local newspapers across the country urging people to protect their SSN and card;
- We broadcast "Tips to Prevent Identity Theft" on our field offices' TV monitors, which explains how individuals can protect themselves from becoming identity theft victims; and,
- We partner with the Federal Trade Commission to educate the public through local seminars and public information materials.

We created a publicity campaign for the employer community entitled, "*Do You Really Need to See the Card*?" We emphasize that employers do *not* need to see the SSN card. Instead, they can quickly verify if the employee's name and SSN match our records using our free SSN

verification services. We regularly speak to the employer community, work with payroll and tax stakeholders, produce publications, and provide SSN-related information on our website.

We stress to employers and payroll professionals the importance of keeping the Social Security card and number safe and secure.

We work with the American Association of Motor Vehicle Administrators, National Association of Motor Vehicle Boards and Commissions, American Association of University Administrators, and the American Association of Collegiate Registrars and Admissions Officers to decrease and limit the use and display of the SSN on drivers' licenses or as student identifiers.

In 2010, we joined the National Cybersecurity Alliance led by DHS. This group works to increase public awareness of cybersecurity and decrease identity theft by sharing knowledge and resources among Federal agencies.

4) If someone knows their SSN has been stolen or compromised, but no actual fraud has occurred to date, can the individual apply for a new number? What guidelines does the SSA follow for when a replacement card is issued? Can the SSA help an individual protect a stolen number?

When a member of the public contacts us regarding identity theft, we take immediate action to assist them:

- We verify the accuracy of our record of the individual's reported earnings.
- We issue a replacement card with the same number if the individual's SSN card has been stolen.
- We consider assigning a new SSN if the victim requests a new SSN, and we determine the person has been harmed by misuse of the SSN.
- We provide publications such as, *Identity Theft and Your Social Security Number* and the above mentioned, *Your Social Security Number and Card*.
- We refer the individual to the FTC, which will assist the individual in placing a fraud alert with the major credit reporting bureaus (Equifax, Experian, and TransUnion), closing financial accounts, and filing necessary reports with the police.
- We refer cases of identity theft to our Office of the Inspector General (OIG). OIG will work with the United States Attorney to determine whether to prosecute the person misusing the SSN.
- We advise tax fraud victims to contact the Internal Revenue Service.

We will assign a new SSN if we determine:

- that misuse has taken place;
- there is documentation, such as a police report, of the misuse;
- the misuse was committed with criminal or harmful intent;
- the misuse has caused the individual to be personally or economically disadvantaged; and,
- the individual has been disadvantaged by the misuse within the past year.

An individual requesting a new SSN must prove age, U.S. citizenship or lawful immigration status, and identity.

An individual should consider changing his or her SSN only as a last resort. Because of the widespread use of the SSN, getting a new SSN may adversely affect a person's ability to interact with Federal agencies, State agencies, employers, schools, medical institutions, and others, as many of the individual's records may be identified under the former SSN. An individual who obtains a new SSN will have to notify banks, schools, medical institutions, etc., so that records can be properly tracked and cross-referenced. Since a new SSN can also be stolen, assigning a new SSN is not a guaranteed solution to identity theft.

We will not assign a new SSN:

- to avoid the consequences of filing for bankruptcy;
- to avoid the law or legal responsibility; or
- if no evidence exists that another person is using that number.

5) The Subcommittee is interested in removing the SSN from the Medicare card and inserting another identifying number for Medicare use, much like the military is doing with its ID cards. The SSA systems would not have to make any changes except interfacing with the Centers for Medicare and Medicare Services to identify the new number with the correct SSN already in their system. Is this the simplest way to alter the system, and if so, what are the costs and the time frames for achieving the change?

We defer to CMS with respect to the analysis of the Subcommittee's idea, costs, and timeframes. The specific effects on our systems, including costs and timeframes, would be dependent on CMS specifications to remove the SSN from the Medicare card.

We appreciate the importance of addressing potential identity theft and fraud issues. Nevertheless, we must balance the benefits of removing the SSN from the Medicare card against the additional resources required to do so. We expect that any proposal would require changes to our systems and would increase visits to our field offices and calls to our toll-free number. Congress cut $1 billion from our fiscal year 2011 budget request, and we are concerned about our resource ability to implement changes.

6) As you may know, the Department of Education recently proposed a rule known as the "gainful employment" ruling that would limit the use of Title IV funding at proprietary, or for-profit, colleges. This rule would employ a formula based on a student's debt and income to determine whether students at these schools meet the Department's definition of holding gainful employment after graduation. Many Members of Congress have concerns with this rule, as evidenced by the 289 votes in the U.S. House of Representatives in favor of an amendment to block Fiscal Year 2011 funding for the implementation of this rule. One of my concerns is the use of SSNs to collect confidential taxpayer date to determine whether or not graduates are earning what the government has defined as gainful income in order for their degree program to maintain eligibility for Title IV funding.

What is the SSA doing to protect students and schools from data loss and theft? What assurances can be provided that this new system of records will not be exposed to cyber security risks, privacy risks or be subject to law enforcement or national security investigatory demands for information? In other words, has a privacy and data security impact assessment been done and, if so, what were the findings?

The IRS owns tax return data. Our authority to use and share tax return data for disclosure purposes is subject to section 6103 of the *Internal Revenue Code* (IRC).

We will provide strictly statistical aggregate data, including mean and median calculations, to the Department of Education (DOE). These data will not contain any information on individual taxpayers, and we will not identify any taxpayer, either directly or indirectly. As such, the data we will provide is not tax return information protected by section 6103 and our use will fully comply with the requirements of the IRC. The *E-Government Act of 2002* requires agencies to conduct privacy impact assessments (PIA) for new electronic information systems and collections containing PII and make them publicly available. Since we are not collecting or sharing new PII in this instance, we do not need to conduct a PIA.

We discussed our proposal for providing aggregate data to DOE with IRS Counsel before preparing the reimbursable agreement. We plan to use the taxpayer identifying information we receive from DOE to match our records and perform an electronic data exchange in accordance with all applicable privacy and security laws and regulations. Once we draft the data exchange agreement, we will share the agreement with IRS Counsel to ensure that we comply with all provisions of the IRC.

7) As you know identity theft is one of the fastest growing crimes in America, and one of the reasons for this is the ease of finding SSNs on unprotected documents. In many states, each foster child is issued an identity card with his or her SSN on the card and the SSN is used as the primary identifier of the child. The federal government allows for a SSN change when a foster child is going through the adoption process. A new SSN largely cleans the financial slate for these children. Is issuing a new SSN a solution for minors, such as foster youth, who have been victims of identity theft? What is the impact of issuing a new SSN?

With respect to identity theft, our treatment of minors is identical to our treatment of adults. Please see our answer to question 4 above.

8) When a person uses an SSN to apply for credit or open an account, what mechanisms are there for the creditor to check the legitimacy of the SSN and whether or not it belongs to a minor? Would it raise a red flag if a creditor discovered the SSN belonged to a minor? Do creditors routinely check to determine if an SSN belongs to a minor?

We offer a fee and consent-based verification service, Consent Based SSN Verification (CBSV), which provides instant, automated verification to enrolled private companies. Using CBSV,

participating companies can confirm that a name, SSN, and date of birth match information in our records.

Because this is a consent-based service, a company must have written permission from the number-holder to conduct the match. We charge a fee to cover the costs of this service because it does not relate to the administration of our programs. Of the 153 companies currently enrolled, 72 companies have used CBSV since 2008. Based on the information contained in each company's profile, 66 companies identified themselves as "Mortgage/Banking Services" as the reason for using CBSV.

Regarding the issuance of credit to minors, we do not have any oversight of the financial industry. The Federal Reserve Board, the Consumer Financial Protection Bureau, and other agencies responsible for the banking industry have oversight in this matter.

9) As a result of setting a limit with respect to the number of Social Security cards an individual can have, there has been an increase in the number of individuals coming into field offices asking for printouts of SSNs, also known as "Numi-Lites." What are your thoughts on charging individuals for these printouts both as a way to cover costs and discourage individuals and businesses from requesting them? Is it also true that the SSA requires less proof of identity for the print outs than for a new Social Security card?

The Freedom of Information Act requires us to provide copies of our records to number-holders upon request. The main reason individuals request printouts is because an employer has requested such a document. We may consider charging a fee for the printout in the future, but current statutory language does not allow us to charge a fee for this service.

We require an individual to submit certain documents as proof of identity for an SSN card. An acceptable document must be current (not expired) and show the person's name, identifying information, and preferably a recent photograph. We will not issue an original SSN card without proper evidence of identity, age, and citizenship. In the case of noncitizens, we also require proof of work authorization.

When an individual requests a "NUMI-Lite" or any other information, the requester must provide the SSN and establish his or her identity by supplying certain identifying information. We compare the information provided to us with information in our records. These evidence requirements provide sufficient proof to release information to the individual.

10) When it comes to enumerating foreign workers, why does the SSA not issue SSNs to temporary workers? Why are SSNs that are issued for work authorization not rescinded or suspended when the non-citizen leaves the country?

The *Social Security Act*[1] requires us to issue SSNs to aliens with work authorization, regardless of the duration of the work authority. The SSN cards we issue to foreign workers with

[1] Section 205(c)(2)(B)(i)(I).

temporary work authority bear the restrictive legend "valid for work with DHS authorization" on the face of the card.

We issue SSNs in order to keep track of workers' earnings and to correctly calculate and pay benefits. Under totalization agreements, temporary workers may become eligible for benefits based, in part, on earnings in the U.S. long after they have left the U.S., just as U.S. citizens may receive benefits based, in part, on work they performed outside the U.S.

The SSN does not provide work authorization, only documents issued by DHS can provide such authority to a non-citizen. DHS can extend work authority for a non-citizen and DHS determines when a non-citizen must leave the country.

11) More children, and in fact, unborn children are having their identities stolen because thieves have figured out the algorithm SSA uses to generate the numbers. SSA is changing this now. Why can't SSA issue a new number to a child?

Please see our answer to question 4 above with respect to issuing a new SSN to a child. Our treatment of children is identical to our treatment of adults.

As you note, we are randomizing the SSN assignment process. Through randomization, we can include previously excluded area numbers and thus increase the pool of SSNs available for assignment from 288 million to 422 million. We also believe randomization will impede reconstructing an individual's SSN.